

FILED

AO 106 (Rev. 04/10) Application for a Search Warrant

AUTHORIZED AND APPROVED/DATE: _____

UNITED STATES DISTRICT COURT

for the

Western District of Oklahoma



4:09 pm, May 01, 2023

CARMELITA REEDER SHINN, CLERK
U.S. DIST. COURT, WESTERN DIST. OKLA.

By: Carrie James, Deputy Clerk

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)A red Apple iPhone, model 11, IMEI: 356561108917767,
currently in the possession of HSI Oklahoma City

Case No. M-23 -274- -STE

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

located in the Western District of Oklahoma, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. 841(a)	Possession with Intent to Distribute and Distribution of Cocaine
21 U.S.C. 846	Drug Conspiracy

The application is based on these facts:

See the attached Affidavit of HSI Special Agent Ryan Belcher.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

RYAN BELCHER, Special Agent, HSI

Printed name and title

Sworn to before me and signed in my presence.

Date: May 1, 2023City and state: Oklahoma City, Oklahoma

Judge's signature

SHON T. ERWIN, U.S. MAGISTRATE JUDGE

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF OKLAHOMA

**IN THE MATTER OF THE SEARCH OF
A RED APPLE IPHONE, MODEL 11,
IMEI: 356561108917767, CURRENTLY
LOCATED AT THE HSI OKLAHOMA
CITY OFFICE**

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Ryan Belcher, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of an electronic device which is a red Apple iPhone (**Target Device**), as further described in Attachment A, to extract from that property electronically stored information described in Attachment B.

2. I am a Special Agent with Homeland Security Investigations (“HSI”) and have been so employed since April 2015. I am presently assigned to the HSI office in Oklahoma City, Oklahoma (hereinafter referred to as HSI OKC).

3. I am an investigative or law enforcement officer who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in 18 U.S.C. § 2516. I am authorized to conduct criminal investigations of violations of the laws of the United States and to execute warrants issued under the authority of the United States.

4. I have been involved in a wide variety of investigative matters. Among other responsibilities, I am responsible for conducting investigations into violations of federal criminal laws, including the manufacturing and possession of controlled substances with the intent to distribute. I have received approximately 24 weeks of specialized training at the Federal Law Enforcement Training Center in the enforcement of federal laws. I have arrested, interviewed, and debriefed numerous individuals who have been involved and have personal knowledge of transporting and concealing narcotics, as well as, the amassing, spending, converting, transporting, distributing, money laundering and concealing of proceeds from narcotics trafficking and smuggling. I have participated in numerous investigations involving physical and electronic surveillance. I have testified in judicial proceedings concerning the prosecution for violations of laws related to the smuggling and trafficking of contraband, including controlled substances. I have been the affiant and participated on numerous federal search warrants.

5. The facts in this Affidavit are based upon my personal observations, my training and experience, reports provided to me by other law enforcement officers, and statements made by witnesses and other concerned parties. Since this Affidavit is being submitted for the limited purpose of establishing probable cause for the requested warrant, I have not included each and every fact known to me concerning this investigation.

6. The Court has jurisdiction to issue the proposed warrant because it is a “court of competent jurisdiction” as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated. *See* 18 U.S.C. § 2711(3)(A)(i).

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

7. The property to be searched is a red Apple iPhone, Model 11, IMEI 356561108917767, hereinafter the “**Target Device**.” The **Target Device** is currently located in secure evidence storage at the HSI OKC office. The **Target Device** is described in more detail in **Attachment A** hereto. Based on the facts set forth below, I believe there is probable cause to believe that the **Target Device** contains evidence of violations of 21 U.S.C. § 841(a), more specifically distribution of cocaine and possession with intent to distribute cocaine, and 21 U.S.C. § 846, a drug conspiracy to do the same, as described further in **Attachment B** (description of items to be seized).

8. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in **Attachment B**.

PROBABLE CAUSE

9. HSI OKC, the Oklahoma Bureau of Narcotics (OBN), and the Lawton Police Department (LPD) are currently conducting a joint investigation targeting ISAIAH CLINTON MCGILL (MCGILL), a cocaine distributor based in Lawton, Oklahoma who has distribution activities that extend through Oklahoma City, Oklahoma and likely up to Missouri. The investigation began in mid-2021, and by utilizing cooperating defendants, undercover agents (UC), pole cameras, controlled purchases, Facebook search warrants, pen registers with trap and trace capabilities, ping warrants, GPS trackers on automobiles, and subpoenas for financial documents, agents confirmed that MCGILL distributes cocaine. From January 2022 through November 2022, HSI and OBN conducted eleven

(11) controlled purchases of cocaine from MCGILL, primarily at the businesses he owned throughout Lawton, Oklahoma.¹ On January 3, 2023, MCGILL was indicted, along with six co-defendants, in case number CR-23-008-JD. The owner and user of the **Target Device** was co-defendant Jennifer Simpson (SIMPSON).

10. During this investigation, law enforcement identified MCGILL as the subscriber and user of phone number (580) 678-4101. On November 7, 2022, HSI Oklahoma OKC presented, and was later granted, through a United States District Judge in the Western District of Oklahoma, an order authorizing the interception of wire communications for (580) 678-4101 (TT1). Through the use of that wiretap, as well as other investigative methods outlined above, such as the execution of Facebook warrants, use of confidential sources, and controlled buys using undercover agents, investigators learned that MCGILL was trafficking cocaine.

11. On April 22, 2022, MCGILL sent his courier, and now co-defendant, Jennifer SIMPSON (SIMPSON), to pick up 2 kilograms of cocaine from a courier delivering to Oklahoma City. Agents learned from social media, that SIMPSON worked for MCGILL at one of his smoke shops. The delivery was a controlled delivery set up by DEA El Paso after they intercepted the drugs coming from Mexico. SIMPSON arrived at the exchange and accepted the suspected cocaine. Unbeknownst to SIMPSON, DEA agents had

¹ MCGILL owned BLVD smoke shops, and the Dragon West topless nightclub.

swapped the real cocaine for “sham” drugs prior to the controlled delivery. SIMPSON picked up the drugs at approximately 6:30 p.m.

12. Once SIMPSON accepted the package, she proceeded south towards Lawton before she was pulled over by the Oklahoma Highway Patrol (OHP). During the stop, an officer ran his dog around the vehicle and told SIMPSON that the dog had alerted to the presence of drugs in the car. When the trooper asked SIMPSON if there were drugs in the car, she responded affirmatively. SIMPSON also had a chamber loaded 9mm pistol in the vehicle and her child was also with her. The trooper recovered the package delivered to her during the controlled delivery that contained the sham drugs.

13. Agents had an active pen register for MCGILL’S phone and eventually learned that phone number (580) 951-0255 was in contact with MCGILL 7 times on April 22, 2022, from 2:15 pm. to 6:36 p.m. When agents subpoenaed the T-Mobile phone records for the number (580) 951-0255, they learned that the number was subscribed to and used by SIMPSON.

14. On January 3, 2023, a federal arrest warrant was issued for the arrest of SIMPSON. On January 13, 2023, SIMPSON was arrested by the Comanche County Sheriff’s Office. SIMPSON was arrested outside of her residence and once she was detained, she asked the deputies if they would get her cell phone (**Target Device**) from inside the residence. During SIMPSON’S booking into the Comanche County jail, as she was providing her biographical data, she listed (580) 951-0255 and her contact number.

15. In light of these facts, especially the calls between the two near in time to suspected drug activity, I believe there is probable cause that the **Target Device** contains evidence of violations of 21 U.S.C. § 841(a) and 21 U.S.C. § 846 as further described in **Attachment B**.

BACKGROUND REGARDING CELLULAR DEVICES

16. Based upon my training and experience, I am aware that individuals involved with drug trafficking often use cell phones and other similar electronic devices, such as tablets, and computers to maintain contact with other co-conspirators, including suppliers, transporters, distributors, and purchasers of illegal narcotics. Such devices and their associated memory cards commonly contain electronically stored information which constitutes evidence, fruits, and instrumentalities of drug trafficking offenses including, but not limited to, the phone directory and/or contacts list, calendar, text messages, e-mail messages, call logs, photographs, and videos. Based upon my training and experience, I know that most drug trafficking, particularly high-level drug trafficking, is coordinated via cell phones and similar electronic devices. Conspirators use these devices to make requests for drug purchases, provide information on price, and set up places to meet for transactions. Consequently, the cellular telephones and similar electronic devices of individuals involved in this drug conspiracy will likely contain evidence of such illegal activity. Therefore, I submit that there is probable cause to believe that the **Target Device** contains evidence of violations of 21 U.S.C. § 841(a) and 21 U.S.C. § 846 as further described in **Attachment B**.

TECHNICAL TERMS

17. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. **Wireless telephone:** A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. **Digital camera:** A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images.

Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each

satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
- f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series

of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

18. Based on my training, experience, and research, I know that the **Target Device** has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, internet outlet with IP Address, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

19. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

20. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file.
- b. Forensic evidence on a device can also indicate who has used or controlled the Device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on the Device is evidence may depend on other information stored on the Device and the application of knowledge about how the Device operates.

Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a Device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

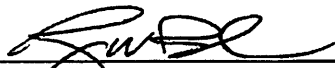
21. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

22. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

23. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the **Target Device** described in **Attachment A** to seek the items described in **Attachment B**.

Respectfully submitted,



RYAN BELCHER
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me on May 1, 2023



SHON T. ERWIN
United States Magistrate Judge

ATTACHMENT A

The property to be searched is a red Apple iPhone, model 11, and IMEI 356561108917767 unknown (**Target Device**). The **Target Device** is currently located in secure evidence storage at the HSI Oklahoma City office.



ATTACHMENT B

Particular Things to be Seized

1. All evidence relating to violations of 21 U.S.C. § 841(a) and 21 U.S.C. § 846, including but not limited to:
 - a. Any and all images, videos, and any other digital media content of SIMPSON and/or his co-conspirators, relating to assets, or illegal drugs;
 - b. call logs, address books, GPS data, internet access, IP accounts, text messages, and email accounts;
 - c. lists of customers and related identifying information;
 - d. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
 - e. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
 - f. any information recording SIMPSON’S schedule or travels from January 2022, which correlates to the timeframe of the first controlled purchases using an undercover agent, through January 13, 2023, the date of her arrest;
 - g. all bank records, checks, credit card bills, account information, and other financial records.
2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records documenting the use of the Internet Protocol addresses to communicated with e-mail servers, internet sites, and social media, including:
 - a. records of Internet Protocol addresses used;
 - b. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

4. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied, or disclosed pursuant to this warrant in order to locate any evidence, fruits, and instrumentalities of violations of the above-listed federal criminal statutes. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.